REMARKS

Claims 1-20 are pending in this application. No claim amendments have been made.

Request for Continued Examination

Applicants submit herewith a Request for Continuing Examination (RCE) in order to ensure consideration of the IDS submitted herewith.

Information Disclosure Statement

The Information Disclosure Statement submitted herewith lists the US Published Application 2003/0005218 A1 to Takano (U.S. '218), which is the US equivalent to JP 2002-24494, which is also listed on the PTO-1449 form. U.S. '218 claims priority from the listed Japan patent application and also from three other Japan priority applications. Only one of the Japan priority applications is listed in the PTO-1449 form is cited by Applicants. Consideration of the references is respectfully requested.

Examiner Interview

Applicants extend their appreciation to the Examiner for granting a Personal Interview with the undersigned and Mr. Hiroshi Kawano who is a member of the assignee of the present invention, Hitachi, Ltd. In the interview, the differences between the invention as claimed and the Sanada et al. publication were discussed. In particular, Figure 2 of the present application, which shows an access controlling table 123, was discussed in comparison to Fig. 8 of the Sanada et al. publication. No agreement was reached in the Interview as to the allowability of the claims. The entirety of Applicants' arguments asserting allowability of the claims is presented herein. Further, as indicated in the Interview, an RCE is filed with this reply in order to have an IDS considered.

Claim Rejections under 35 U.S.C. §§102 and 103

Claims 1-8 and 12-20 are rejected under 35 U.S.C. §102(b) as being anticipated by Sanada et al., U.S. Publication No. 2001/0008010 (hereinafter Sanada); and claims 9-10 are rejected under 35 U.S.C. §103(a) as being unpatentable over Sanada in view of Li et al., U.S. Publication No. 23003/0093509. Reconsideration of the rejections is respectfully requested for the following reasons.

As recognized by Applicants, the present invention relates to ensuring the security of data stored in a second storage system 101 (Fig. 1) connected to networks 107 and 108. In particular, when a second storage system is directly connected to a network, there is a possibility that an unspecified number of host computers can gain access to the hard disk drives of the second storage system. Accordingly, access is controlled in the present invention by determining which I/O commands are authorized between a plurality of network transportation ports of the second storage system and the hard disk drives (103, 104, 105, etc.) of the second storage system.

Claim 1, for example, sets forth that the controller of the second storage system has an access controller having an access controlling table for storing access control setting information which defines the I/O commands that are to be authorized between each of the plurality of transportation ports 113, 114 and each of the plurality of nonvolatile data storing means (103, 104, etc.). An internal network 106 connects the disk controller with the nonvolatile data storing means and networks (working group 1 (107) and working group 2 (108)) are connected to respective host computers and to network transportation ports 113, 114 of the disk controller. The disk controller 102 receives and interprets I/O commands requested by the host computers 109 to 112, and converts them into a proper form, to issue to the hard disk drives 103 to 105. In particular, the access controllers (access control units 115, 116) interpret and execute I/O requests transmitted by the host computers such that when an I/O process is transmitted, the access controllers refer to an access controlling table (123) that stores access authorization setting information in order to determine whether the I/O commands should be authorized between each of the plurality of transportation ports (113, 114) and each of the plurality of nonvolatile data storing means (103, 104, etc.).

As shown in detail in FIG. 2 of the present application, access controlling information is set in the access controlling table 123. The access authorization setting for each logical disk (201, 202 ... 203) is described in the columns of the example for each network port (204, 205). The table 123 of Fig. 2 shows I/O commands in which access from the network ports is authorized for each logical disk. For example, the authorized I/O commands from the network port 0 for the logical disk 201 are described as "READ enable," "WRITE enable", whereas the there are no I/O commands recognized from the network port 1 for the logical disk 202, and therefore an I/O command to virtual disk 202 through network port 1 is not recognized by the host computer connected to such network port, i.e. access from the network port is recognition-disabled. See page 11, lines 12-22 of the specification, for example. Accordingly, unauthorized access from any host computer connected to port 1 is not possible with respect to logical disk 202.

Further, with reference to Fig. 3, when the second storage system 101 receives and executes I/O commands from the host computer that reach the network ports of the second storage device, they are transmitted to the corresponding access controllers 115 and 116. The access controllers 115 and 116 extract a target logical disk number included in the I/O commands and refer to the access controlling table 123 via the table controller 125. The access controller reads contents of a corresponding field of the access controlling table from the logical disk number and the identifier of the network port and judges whether or not such I/O command is authorized. If it is authorized, then the I/O command is execute and if not, the access controllers 115 and 116 notify the host computer of a failure of the I/O command.

Sanada is relied upon for disclosing a controller having a plurality of network transportation ports connected to different networks and an access controller for processing I/O commands requested for the transportation ports, including an access controlling table for storing access control setting information which defines the I/O commands that are to be authorized between each of the plurality of transportation ports and each of the plurality of nonvolatile data storing devices. However, the control table 140, shown in Fig. 8 of Sanada, stores information used in determining whether access is authorized between the logical units and the hosts. Of course, ports are provided through which the I/O commands are

transmitted, but in Sanada the access is controlled on the basis of authorization provided between hosts and logical units, not logical units and ports, as in the present invention.

In greater detail, the control table 140 of Sanada includes port identifier information, such as N_Port_Name, which identifies the host (paragraph 0079). Further, the host computers transmit a frame including the N_Port_Name and a LUN that is matched with like information in the control table. For example, when a SCSI command is received, it is first acknowledged by the controller, and then the N_Port_Name and LUN information stored in the frame are extracted and the table 140 is used to determine if the host computer can access the LUN that is specified (paragraph 0108). If table information includes the host information, e.g. HOSTA or HOSTB for the LUN that is specified, then access is permitted to the specified LUN and the I/O processing is continued. On the other hand, if the combination of the N_Port_Name and corresponding LUN are not present in the control table 140 (after a search is conducted), the SCSI command is rejected by the controller (paragraphs 0110 - 0115). Therefore, authorization of I/O in Sanada is performed on the basis of a relationship preset in the control table between the hosts (N_Port_Name) and the LUNs. Accordingly, the rejection of claims 1-8 and 12-20 under 35 U.S.C. §102(b) should be withdrawn.

Li is relied upon for disclosing the steps of claims 9 and 10, wherein when a frequency of judgment that access non-authorization to specific data stored in the nonvolatile data storing means exceeds a predetermined threshold, access from the plurality of transportation ports to the data is not authorized. However, Li does not make up for the deficiency in Sanada with respect to the invention set forth in the independent claims, as aforementioned. Accordingly, the combination of Sanada and Li does not render the invention set forth in claims 9 and 10 unpatentable under 35 USC §103(a).

CONCLUSION

In view of the foregoing, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

By _____
John R. Mattingly
Reg. No. 30,293
(703) 684-1120

JRM/so
Date: March 9, 2006